

An extremal even unimodular lattice of dimension 72

Gabriele Nebe

Lehrstuhl D für Mathematik

KOLKOM, Saarbrücken, November 2010



Doubly-even self-dual codes

Definition

- ▶ A linear binary **code** C of length n is a subspace $C \leq \mathbb{F}_2^n$.
- ▶ The **dual code** of C is

$$C^\perp := \{x \in \mathbb{F}_2^n \mid (x, c) := \sum_{i=1}^n x_i c_i = 0 \text{ for all } c \in C\}$$

- ▶ C is called **self-dual** if $C = C^\perp$.
- ▶ The **Hamming weight** of a codeword $c \in C$ is $\text{wt}(c) := |\{i \mid c_i \neq 0\}|$.
- ▶ C is called **doubly-even** if $\text{wt}(c) \in 4\mathbb{Z}$ for all $c \in C$.
- ▶ The **minimum distance** $d(C) := \min\{\text{wt}(c) \mid 0 \neq c \in C\}$.
- ▶ The **weight enumerator** of C is $p_C := \sum_{c \in C} x^{n-\text{wt}(c)} y^{\text{wt}(c)} \in \mathbb{C}[x, y]_n$.

The minimum distance measures the error correcting quality of a self-dual code.

Self-dual codes

Remark

- ▶ The **all-one vector** $\mathbf{1}$ lies in the dual of every even code since $\text{wt}(c) \equiv_2 (c, c) \equiv_2 (c, \mathbf{1})$.
- ▶ If C is self-dual then $n = 2 \dim(C)$ is even and

$$\mathbf{1} \in C^\perp = C \subset \mathbf{1}^\perp = \{c \in \mathbb{F}_2^n \mid \text{wt}(c) \text{ even}\}.$$

- ▶ Self-dual doubly-even codes correspond to totally isotropic subspaces in the quadratic space $\mathbf{1}^\perp / \langle \mathbf{1} \rangle$.

The extended **Hamming code**

$$h_8 : \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

has $p_{h_8}(x, y) = x^8 + 14x^4y^4 + y^8$ and is the unique doubly-even self-dual code of length 8.

Extremal codes

The binary **Golay code** \mathcal{G}_{24} is the unique doubly-even self-dual code of length 24 with minimum distance ≥ 8 .

$$p_{\mathcal{G}_{24}} = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$$

Theorem (Gleason)

Let $C = C^\perp \leq \mathbb{F}_2^n$ be doubly even. Then

- ▶ $n \in 8\mathbb{Z}$
- ▶ $p_C \in \mathbb{C}[p_{h_8}, p_{\mathcal{G}_{24}}]$
- ▶ $d(C) \leq 4 + 4\lfloor \frac{n}{24} \rfloor$

Doubly-even self-dual codes achieving this bound are called **extremal**.

length	8	16	24	32	48	72	80
$d(C)$	4	4	8	8	12	16	16
extremal codes	h_8	$h_8 \perp h_8, d_{16}^+$	\mathcal{G}_{24}	5	QR_{48}	?	≥ 4

Turyn's construction of the Golay code

Construction of Golay code

Choose two copies C and D of h_8 such that

$$C \cap D = \langle \mathbf{1} \rangle, \quad C + D = \mathbf{1}^\perp \leq \mathbb{F}_2^8$$

$\mathcal{G}_{24} := \{(c + d_1, c + d_2, c + d_3) \mid c \in C, d_i \in D, d_1 + d_2 + d_3 \in \langle \mathbf{1} \rangle\}$

(a) $\mathcal{G}_{24} = \mathcal{G}_{24}^\perp$.

(b) \mathcal{G}_{24} is doubly-even.

(c) $d(\mathcal{G}_{24}) = 8$.

Proof: (a) unique expression if c represents classes in $h_8/\langle \mathbf{1} \rangle$, so

$$|\mathcal{G}_{24}| = 2^3 \cdot 2^4 \cdot 2^4 \cdot 2 = 2^{12}$$

Suffices $\mathcal{G}_{24} \subseteq \mathcal{G}_{24}^\perp$: $((c + d_1, c + d_2, c + d_3), (c' + d'_1, c' + d'_2, c' + d'_3)) = 3(c, c') + (c, d'_1 + d'_2 + d'_3) + (d_1 + d_2 + d_3, c') + (d_1, d'_1) + (d_2, d'_2) + (d_3, d'_3) = 0$

(b) Follows since C and D are doubly-even, so generators have weight divisible by 4.

Turyn's construction of the Golay code

Construction of Golay code.

Choose two copies C and D of h_8 such that

$$C \cap D = \langle \mathbf{1} \rangle, \quad C + D = \mathbf{1}^\perp \leq \mathbb{F}_2^8$$

$\mathcal{G}_{24} := \{(c + d_1, c + d_2, c + d_3) \mid c \in C, d_i \in D, d_1 + d_2 + d_3 \in \langle \mathbf{1} \rangle\}$

(c) $d(\mathcal{G}_{24}) = 8$.

Proof: (c)

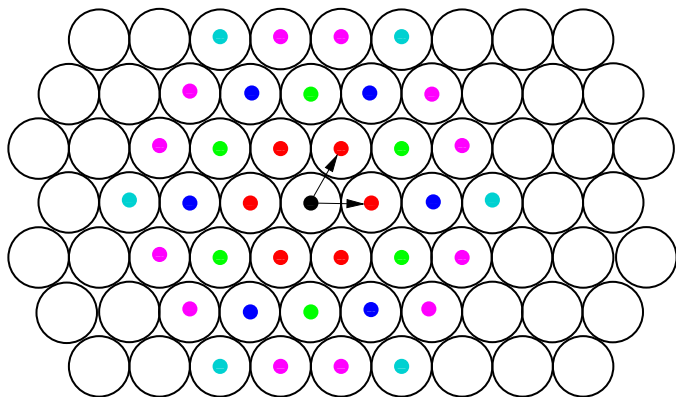
$\text{wt}(c + d_1, c + d_2, c + d_3) = \text{wt}(c + d_1) + \text{wt}(c + d_2) + \text{wt}(c + d_3)$.

- ▶ 1 non-zero component: $(d, 0, 0)$ with $d \in \langle \mathbf{1} \rangle$, weight 8.
- ▶ 2 non-zero components: $(d_1, d_2, 0)$ with $d_1, d_2 \in D \cong h_8$, weight $\geq d(h_8) + d(h_8) = 4 + 4 = 8$.
- ▶ 3 non-zero components: All have even weight, so weight $\geq 2 + 2 + 2 = 6$. By (b) the weight is a multiple of 4, so ≥ 8 .

Turyn applied to Golay

will not yield an extremal code of length 72. Such an extremal code has no automorphism of order 2 which has fixed points.

Lattices and sphere packings



Hexagonal Circle Packing

$$\theta = 1 + 6q + 6q^3 + 6q^4 + 12q^7 + 6q^9 + \dots$$

Dense lattice sphere packings

- ▶ Classical problem to find densest sphere packings:
- ▶ Dimension 2: **Lagrange** (lattices), **Fejes Tóth** (general)
- ▶ Dimension 3: Kepler conjecture, proven by **T.C. Hales** (1998)
- ▶ Dimension ≥ 4 : open
- ▶ Densest **lattice** sphere packings:
- ▶ Voronoi algorithm (~ 1900) all locally densest lattices.
- ▶ Densest lattices known in dimension 1,2,3,4,5, **Korkine-Zolotareff** (1872) 6,7,8 **Blichfeldt** (1935) and **24 Cohn, Kumar** (2003).
- ▶ Density of lattice measures error correcting quality.

Even unimodular lattices

Definition

- ▶ A **lattice** L in Euclidean n -space $(\mathbb{R}^n, (\cdot, \cdot))$ is the \mathbb{Z} -span of an \mathbb{R} -basis $B = (b_1, \dots, b_n)$ of \mathbb{R}^n

$$L = \langle b_1, \dots, b_n \rangle_{\mathbb{Z}} = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in \mathbb{Z} \right\}.$$

- ▶ The **dual lattice** is

$$L^{\#} := \{x \in \mathbb{R}^n \mid (x, \ell) \in \mathbb{Z} \text{ for all } \ell \in L\}$$

- ▶ L is called **unimodular** if $L = L^{\#}$.
- ▶ $Q : \mathbb{R}^n \rightarrow \mathbb{R}_{\geq 0}$, $Q(x) := \frac{1}{2}(x, x)$ **associated quadratic form**
- ▶ L is called **even** if $Q(\ell) \in \mathbb{Z}$ for all $\ell \in L$.
- ▶ $\min(L) := \min\{Q(\ell) \mid 0 \neq \ell \in L\}$ **minimum** of L .

The **sphere packing density** of an even unimodular lattice is proportional to its minimum.

Lattices and codes

Construction A

Let (e_1, \dots, e_n) be an orthogonal basis of \mathbb{R}^n with $Q(e_i) = 1$ for all i .
Let $C \leq \mathbb{F}_2^n$ be a code. Then

$$L_C := \left\{ \sum_{i=1}^n \frac{a_i}{2} e_i \mid (a_1 + (2), \dots, a_n + (2)) \in C \right\} \subset \mathbb{R}^n$$

is called the **codelattice** of C .

Duality

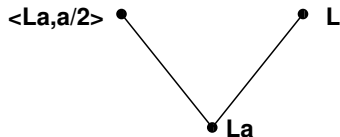
- ▶ $L_C^\# = L_{C^\perp}$
- ▶ L_C is even, if C is doubly-even
- ▶ L_C is even unimodular, if C is self-dual and doubly-even.

$L_{h_8} = E_8$ the unique even unimodular lattice of dimension 8.

The Leech lattice and the Golay code

Construct an even unimodular lattice $\Lambda_{24} \leq \mathbb{R}^{24}$ with minimum 2 from the Golay code.

- ▶ Let $L := L_{\mathcal{G}_{24}}$ be the codelattice of the Golay code.
- ▶ Then L is an even unimodular lattice and $\{\pm e_1, \dots, \pm e_{24}\} = \{v \in L \mid Q(v) = 1\}$.
- ▶ Let $a := \frac{3}{2}e_1 + \frac{1}{2}e_2 + \dots + \frac{1}{2}e_{24}$.
- ▶ Then $Q(\frac{1}{2}a) = 2$.
- ▶ Let $L_a := \{v \in L \mid (v, a) \in 2\mathbb{Z}\}$ and
- ▶ $\Lambda_{24} := L^{(a)} := \langle \frac{1}{2}a, L_a \rangle$. Then $\min(\Lambda_{24}) = 2$.



Theta-series of lattices

Let (L, Q) be an even unimodular lattice of dimension n so a regular positive definite integral quadratic form $Q : L \rightarrow \mathbb{Z}$.

- ▶ The **theta series** of L is

$$\theta_L = \sum_{\ell \in L} q^{Q(\ell)} = 1 + \sum_{k=\min(L)}^{\infty} a_k q^k$$

where $a_k = |\{\ell \in L \mid Q(\ell) = k\}|$.

- ▶ θ_L defines a holomorphic function on the upper half plane by substituting $q := \exp(2\pi iz)$.
- ▶ Then θ_L is a modular form of weight $\frac{n}{2}$ for the full modular group $\mathrm{SL}_2(\mathbb{Z})$.
- ▶ n is a multiple of 8.
- ▶ $\theta_L \in \mathcal{M}_{\frac{n}{2}}(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}[E_4, \Delta]_{\frac{n}{2}}$ where $E_4 := \theta_{E_8} = 1 + 240q + \dots$ is the normalized Eisenstein series of weight 4 and

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + \dots \text{ of weight 12}$$

Extremal modular forms

Basis of $\mathcal{M}_{4k}(\mathrm{SL}_2(\mathbb{Z}))$:

$$\begin{aligned} E_4^k &= 1 + 240kq + *q^2 + \dots \\ E_4^{k-3} \Delta &= q + *q^2 + \dots \\ E_4^{k-6} \Delta^2 &= q^2 + \dots \\ &\vdots \\ E_4^{k-3m_k} \Delta^{m_k} &= \dots q^{m_k} + \dots \end{aligned}$$

where $m_k = \lfloor \frac{n}{24} \rfloor = \lfloor \frac{k}{3} \rfloor$.

Definition

This space contains a unique form

$$f^{(k)} := 1 + 0q + 0q^2 + \dots + 0q^{m_k} + a(f^{(k)})q^{m_k+1} + b(f^{(k)})q^{m_k+2} + \dots$$

$f^{(k)}$ is called the **extremal modular form** of weight $4k$.

$$f^{(1)} = 1 + 240q + \dots = \theta_{E_8}, \quad f^{(2)} = 1 + 480q + \dots = \theta_{E_8}^2,$$

$$f^{(3)} = 1 + 196,560q^2 + \dots = \theta_{\Lambda_{24}},$$

$$f^{(6)} = 1 + 52,416,000q^3 + \dots = \theta_{P_{48p}} = \theta_{P_{48q}} = \theta_{P_{48n}},$$

$$f^{(9)} = 1 + 6,218,175,600q^4 + \dots = \theta_{\Gamma}.$$

Extremal even unimodular lattices

Theorem (Siegel)

$a(f^{(k)}) > 0$ for all k and $b(f^{(k)}) < 0$ for large k ($k \geq 5200$).

Corollary

Let L be an n -dimensional even unimodular lattice. Then

$$\min(L) \leq 1 + \lfloor \frac{n}{24} \rfloor = 1 + m_{n/8}.$$

Lattices achieving this bound are called **extremal**.

Extremal even unimodular lattices $L \leq \mathbb{R}^n$

n	8	16	24	32	40	48	72	80
$\min(L)$	2	2	4	4	4	6	8	8
number of extremal lattices	1	2	1	$\geq 10^7$	$\geq 10^{51}$	≥ 3	≥ 1	≥ 4

Extremal even unimodular lattices in jump dimensions

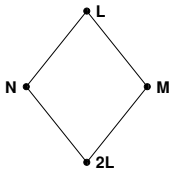
$$f^{(3)} = 1 + 196,560q^2 + \dots = \theta_{\Lambda_{24}}.$$

$$f^{(6)} = 1 + 52,416,000q^3 + \dots = \theta_{P_{48p}} = \theta_{P_{48q}} = \theta_{P_{48n}}.$$

$$f^{(9)} = 1 + 6,218,175,600q^4 + \dots = \theta_{\Gamma}.$$

Let L be an extremal even unimodular lattice of dimension $24m$ so $\min(L) = m + 1$

- ▶ All non-empty layers $\emptyset \neq \{\ell \in L \mid Q(\ell) = a\}$ form spherical 11-designs.
- ▶ The density of the associated sphere packing realises a local maximum of the density function on the space of all $24m$ -dimensional lattices.
- ▶ If $m = 1$, then $L = \Lambda_{24}$ is unique, Λ_{24} is the **Leech lattice**.
- ▶ The 196560 minimal vectors of the Leech lattice form the unique tight spherical 11-design and realise the maximal kissing number in dimension 24.
- ▶ Λ_{24} is the densest 24-dimensional lattice (**Cohn, Kumar**).
- ▶ For $m = 2, 3$ these lattices are the densest known lattices and realise the maximal known kissing number.



Turyn's construction

- ▶ Let (L, Q) be an even unimodular lattice of dimension n .
- ▶ Choose sublattices $M, N \leq L$ such that $M + N = L$, $M \cap N = 2L$, and $(M, \frac{1}{2}Q)$, $(N, \frac{1}{2}Q)$ even unimodular.
- ▶ Such a pair (M, N) is called a **polarisation** of L .
- ▶ For $k \in \mathbb{N}$ let $\mathcal{L}(M, N, k) :=$

$$\{(m + x_1, \dots, m + x_k) \in \perp^k L \mid m \in M, x_i \in N, x_1 + \dots + x_k \in 2L\}.$$
- ▶ Define $\tilde{Q} : \mathcal{L}(M, N, k) \rightarrow \mathbb{Z}$,
$$\tilde{Q}(y_1, \dots, y_k) := \frac{1}{2}(Q(y_1) + \dots + Q(y_k)).$$
- ▶ $(\mathcal{L}(M, N, k), \tilde{Q})$ is an even unimodular lattice of dimension nk .

Obtaining Leech from E_8

Theorem (Lepowsky, Meurman; Elkies, Gross)

Let $(L, Q) \cong E_8$ be the unique even unimodular lattice of dimension 8. Then for any polarisation (M, N) of E_8 the lattice $\mathcal{L}(M, N, 3)$ has minimum ≥ 2 .

Note that $\text{Aut}(E_8)$ acts transitively on the polarisations of E_8 .

Proof: Let $y := (y_1, y_2, y_3) \in \mathcal{L}(M, N, 3)$.

All $y_i \neq 0$:

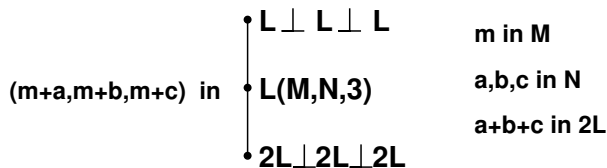
$$\tilde{Q}(y_1, y_2, y_3) = \frac{1}{2} \sum_{i=1}^3 Q(y_i) \geq \lceil \frac{3}{2} \rceil = 2.$$

$y_1 \neq 0 \neq y_2$: Then $y_i \in N$ and

$$\tilde{Q}(y) \geq 1 + 1 + 0 = 2.$$

Only one $y_i \neq 0$ then $y_i \in 2L$ and $\tilde{Q}(y) \geq 2$.

Turyn's construction for $k = 3$



$$d := \min(L, Q) = \min(M, \frac{1}{2}Q) = \min(N, \frac{1}{2}Q)$$

$$\text{Then } \lceil \frac{3d}{2} \rceil \leq \min(\mathcal{L}(M, N, 3)) \leq 2d.$$

Proof:

$$(a, 0, 0) \quad a = 2\ell \in 2L \text{ with } \frac{1}{2}Q(2\ell) = 2Q(\ell) \geq 2d.$$

$$(a, b, 0) \quad a, b \in N \text{ with } \frac{1}{2}Q(a) + \frac{1}{2}Q(b) \geq 2d.$$

$$(a, b, c) \text{ then } \frac{1}{2}(Q(a) + Q(b) + Q(c)) \geq \frac{3}{2}d.$$

72-dimensional lattices from Leech (Griess)

$$\text{If } (L, Q) \cong (M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong \Lambda_{24} \text{ then } 3 \leq \min(\mathcal{L}(M, N, 3)) \leq 4.$$

The vectors v with $Q(v) = 3$

Assume that $(L, Q) \cong (M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong \Lambda_{24}$

- ▶ All 4095 non-zero classes of $M/2L$ are represented by vectors m with $Q(m) = 4$.
- ▶ For $m \in M$ let $N_m := \{a \in N \mid (a, m) \in 2\mathbb{Z}\}$ and $N^{(m)} := \langle N_m, m \rangle$.
- ▶ $(N^{(m)}, \frac{1}{2}Q)$ is even unimodular lattice with root system $24A_1$.
- ▶ $y := (y_1, y_2, y_3) = (m + a, m + b, m + c) \in \mathcal{L}(M, N, 3)$ with $\tilde{Q}(y) = 3$ then $y_i \in N^{(m)}$ are roots and $m + y_1 + y_2 + y_3 \in 2L$.

Enumerate short vectors in $\mathcal{L}(M, N, 3)$

For all 4095 nonzero classes $m + 2L \in M/2L$ and all 24^2 pairs (y_1, y_2) of roots in $N^{(m)}$ check if $\langle 2L, m + y_1 + y_2 \rangle$ has minimum ≥ 3 .

Note that the stabilizer S in $\text{Aut}(L)$ of (M, N) acts. May restrict to orbit representatives $M/2L$.

Closer analysis reduces number of pairs (y_1, y_2) to $8 \cdot 16$.

At most $4095 \cdot 8 \cdot 16 = 524,160$ lattices of dimension 24.

Stehlé, Watkins proof of extremality

Theorem (Stehlé, Watkins (2010))

Let L be an even unimodular lattice of dimension 72 with $\min(L) \geq 3$. Then L is extremal, if and only if it contains at least 6, 218, 175, 600 vectors v with $Q(v) = 4$.

Proof: L is an even unimodular lattice of minimum ≥ 3 , so its theta series is

$$\theta_L = 1 + a_3q^3 + a_4q^4 + \dots = f^{(9)} + a_3\Delta^3.$$

$$f^{(9)} = 1 + 6, 218, 175, 600q^4 + \dots$$

$$\Delta^3 = q^3 - 72q^4 + \dots$$

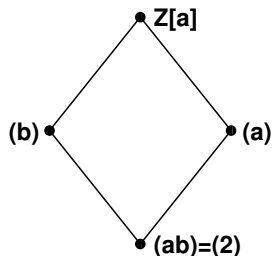
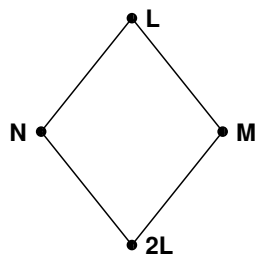
So $a_4 = 6, 218, 175, 600 - 72a_3 \geq 6, 218, 175, 600$ if and only if $a_3 = 0$.

Remark

A similar proof works in all jump dimensions $24k$ (extremal minimum = $k + 1$) for lattices of minimum $\geq k$.

For dimensions $24k + 8$ and lattices of minimum $\geq k$ one needs to count vectors v with $Q(v) = k + 2$.

How to find polarisations



- ▶ Rough estimate shows that there are about 10^{10} orbits of polarisations (M, N) of the Leech lattice such that $(M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong \Lambda_{24}$.
- ▶ Griess proposes $M = (f - 1)L$, $N = (g - 1)L$, $g^2 = f^2 = -1$, (fg) fixed point free odd order: No extremal lattice.
- ▶ Bachoc and Nebe (1995) used Hermitian polarisations to construct extremal 80-dimensional lattices.
- ▶ $\alpha, \beta \in \text{End}(L)$ such that $(\alpha x, y) = (x, \beta y)$ and $\alpha\beta = 2$.
- ▶ $M := \alpha L$, $N := \beta L$.

Hermitian polarisations

Let $\alpha \in \text{End}(L)$ such that

- ▶ $\alpha^2 - \alpha + 2 = 0$ ($\mathbb{Z}[\alpha]$ = integers in $\mathbb{Q}[\sqrt{-7}]$).
- ▶ $(\alpha x, y) = (x, \beta y)$ where $\beta = 1 - \alpha = \bar{\alpha}$.

Then $M := \alpha L$, $N := \beta L$ defines a polarisation of L such that $(L, Q) \cong (M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q)$.

Remark

$\mathcal{L}(\alpha L, \beta L, 3) = L \otimes_{\mathbb{Z}[\alpha]} P_b$ where

$$P_b = \langle (\beta, \beta, 0), (0, \beta, \beta), (\alpha, \alpha, \alpha) \rangle \mathbb{Z}[\alpha]^3$$

with the half the standard Hermitian form

$$h : P_b \times P_b \rightarrow \mathbb{Z}[\alpha], h((a_1, a_2, a_3), (b_1, b_2, b_3)) = \frac{1}{2} \sum_{i=1}^3 a_i \bar{b}_i.$$

P_b is Hermitian unimodular and $\text{Aut}_{\mathbb{Z}[\alpha]}(P_b) \cong \pm \text{PSL}_2(7)$. So $\text{Aut}(\mathcal{L}(\alpha L, \beta L, 3)) \geq \text{Aut}_{\mathbb{Z}[\alpha]}(L) \times \text{PSL}_2(7)$.

Hermitian structures of the Leech lattice

Theorem (M. Hentschel, 2009)

There are exactly nine $\mathbb{Z}[\alpha]$ -structures of the Leech lattice.

	group	order	# $Q(v) = 3$
1	$SL_2(25)$	$2^4 3 \cdot 5^2 13$	0
2	$2.A_6 \times D_8$	$2^7 3^2 5$	$2 \cdot 20,160$
3	$SL_2(13).2$	$2^4 3 \cdot 7 \cdot 13$	$2 \cdot 52,416$
4	$(SL_2(5) \times A_5).2$	$2^6 3^2 5^2$	$2 \cdot 100,800$
5	$(SL_2(5) \times A_5).2$	$2^6 3^2 5^2$	$2 \cdot 100,800$
6	soluble	$2^9 3^3$	$2 \cdot 177,408$
7	$\pm PSL_2(7) \times (C_7 : C_3)$	$2^4 3^2 7^2$	$2 \cdot 306,432$
8	$PSL_2(7) \times 2.A_7$	$2^7 3^3 5 \cdot 7^2$	$2 \cdot 504,000$
9	$2.J_2.2$	$2^9 3^3 5^2 7$	$2 \cdot 1,209,600$

The extremal 72-dimensional lattice Γ

Main result

- ▶ Γ is an extremal even unimodular lattice of dimension 72.
- ▶ $\text{Aut}(\Gamma)$ contains $\mathcal{U} := (\text{PSL}_2(7) \times \text{SL}_2(25)) : 2$.
- ▶ \mathcal{U} is an absolutely irreducible subgroup of $\text{GL}_{72}(\mathbb{Q})$.
- ▶ All \mathcal{U} -invariant lattices are similar to Γ .
- ▶ Γ realises the **densest known sphere packing**
- ▶ and **maximal known kissing number** in dimension 72.
- ▶ Structure of Γ can be used for decoding.

Note that I tried quite a few other polarisations (M, N) of the Leech lattice but did not find other extremal lattices.

Remark (Harada, 2010)

The lattice Γ gives extremal doubly-even codes over $\mathbb{Z}/4k\mathbb{Z}$ of length 72 for $k \geq 2$.

Certain odd neighbors of Γ yield optimal odd unimodular lattices.